
43 Network Security Awareness, Management, and Risk Analysis

HELEN ARMSTRONG

INTRODUCTION

Issues in the management of network security include network security education and awareness, risk analysis, security policies, and other management tasks. At a management level network, security involves consideration of both technological and human factors. The aims of network security are the same for all aspects of IT security including the process control and enterprise networks. The aims of network security include the following:

1. *Confidentiality*: ensures information assets are accessed only by authorized personnel and devices. Confidentiality measures ensure that disclosure of sensitive information is prevented from intentional and unintentional actions.
2. *Availability*: ensures information assets are available when needed by authorized personnel and devices. Measures to ensure availability minimize denial of service actions against systems and information assets.
3. *Integrity*: ensures information assets are modified in authorized ways by authorized people and devices. Integrity measures ensure the reliability and accuracy of information through all stages of its life cycle.
4. *Authentication*: ensures the confirmation and verification that users, devices, and traffic are what they claim to be. Authentications measures ensure unauthorized individuals or devices are denied access to information assets.
5. *Nonrepudiation*: ensures the ability to prove that an individual or device actually carried out a transaction. Nonrepudiation measures ensure that a party in an electronic transaction is not able to deny that it performed an action.

A network may be very secure from a physical perspective; however, the designers, builders, and users of these systems are human, and human behavior can be more unpredictable than that of the equipment or software. Managing network security thus embraces managing the physical environment: the network hardware, software, and data in addition to the humans who use or come into contact with the

network. Network security management covers a broad area and includes the following:

1. Managing network security awareness including security education and developing a security culture
2. Monitoring and managing the entire network environment using a holistic sociotechnological approach
3. Performing risk analysis and risk management and managing security incidents

NETWORK SECURITY AWARENESS

Organizations depend on computer networks to perform many of the functions required for their continued operations and survival. These systems contain a wealth of corporate data and applications and are networked to provide an integrated repository of information-related assets and valuable resources. Employees require an understanding of their role in protecting these important resources. Management needs to ensure that there is a strong security culture within the organization where employees are aware of threats, the impact of these threats, and the security measures employed to minimize their occurrence.

Security Education

Security education provides an effective way of ensuring employees understand important security factors including what is security, why it is needed, how security measures are implemented, who is responsible, and what to do when faced with a security breach. Education for all aspects of network security should be undertaken by every employee upon recruitment and on a regular basis thereafter, with most sensible organizations making this an annual occurrence. Security education ideally covers the objectives of security in the organizational environment, the range of security policies, and the terms of any nondisclosure or employment contract applying to the use of the corporate network and Internet. Security awareness education needs to be tailored to the different groups of participants with appropriate content for the areas of responsibility and levels of decision making.

The *need-to-know* principle should also be applied to groups of employees undertaking the education. This means that the information regarding network security delivered to employees is appropriate to their particular level of access and their need for the knowledge to effectively carry out their jobs.

One of the most important security policies to users is Acceptable Use policy that clearly gives details about the acceptable and nonacceptable behavior together with the implications of noncompliance. This will aid any legal action an organization takes on subsequent noncompliant activities. The education session provides evidence that employers have delivered security training and awareness programs to their staff and are able to present the content of these educational programs to the court if necessary.

Nondisclosure agreements should be signed by all staff at the time of recruitment, and the requirements of these confidentiality agreements can be reinforced at the annual security education sessions. In many cases, organizations will have implemented information classification systems and the education session will include the handling of assets at different levels of sensitivity. In organizations dealing with national security, some computer equipment and networks may also be classified, and relevant staff working with these assets must also be educated in their security.

In leading technology organizations and those dealing with highly sensitive data or equipment such as defense agencies, security educators will often record the questions asked at education sessions and store these on personnel files for potential future investigation of noncompliant activities.

Code of Ethics

A Code of Ethics provides a framework of ethical behavior desired by the management. There are numerous codes of ethics for professionals working in electrical engineering, computer engineering, computer science, and IT, who are members of the associated professional societies. Examples include the IEEE Code of Ethics (see Figure 43.1), Association of Computing Machinery (ACM) Code of Ethics and Professional Conduct (see Figure 43.2), and many codes of ethics from computer societies around the world. These codes are highly appropriate for all employees involved in computing and networking, and can form a starting point for organizations wishing to build a code to suit their own circumstances.

It is recommended that ethical behavior in employees be encouraged and monitored by management. By establishing an ethical standard through a code of ethics and senior management providing a role model, employees will follow the example given. The ACM Code of Ethics is presented in Figure 43.2 and provides another example of a code that would encourage ethical behavior and attainment of high quality standards.

Organizational Security Culture

A security culture where employees are cognizant of network security threats and basic countermeasures is essential to ensure effective security management. Many organizations

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

- To accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
- To avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
- To be honest and realistic in stating claims or estimates based on available data;
- To reject bribery in all its forms;
- To improve the understanding of technology, its appropriate application, and potential consequences;
- To maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
- To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
- To treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
- To avoid injuring others, their property, reputation, or employment by false or malicious action;
- To assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

FIG. 43.1

IEEE Code of Ethics. (From IEEE Computer Society, IEEE ISO/IEC Standard 16085-2006 Systems and Software Engineering—Life Cycle Processes—Risk Management, ISO and IEEE Standards Association, <http://www.ieee.org/> @ (2006) IEEE. Reprinted with permission of the IEEE.)

General moral imperatives

As an ACM member I will ...

- Contribute to society and human well-being.
- Avoid harm to others.
- Be honest and trustworthy.
- Be fair and take action not to discriminate.
- Honor property rights including copyrights and patents.
- Give proper credit for intellectual property.
- Respect the privacy of others.
- Honor confidentiality.

More specific professional responsibilities

As an ACM computing professional I will ...

- Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work
- Acquire and maintain professional competence.
- Know and respect existing laws pertaining to professional work.
- Accept and provide appropriate professional review.
- Give comprehensive and thorough evaluations of computer systems and their impacts including analysis of possible risks.
- Honor contracts, agreements, and assigned responsibilities.
- Improve public understanding of computing and its consequences.
- Access computing and communication resources only when authorized to do so.

Organizational leadership imperatives

As an ACM member and an organizational leader, I will ...

- Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
- Manage personnel and resources to design and build information systems that enhance the quality of working life.
- Acknowledge and support proper and authorized uses of an organization's computing and communications resources.
- Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
- Articulate and support policies that protect the dignity of users and others affected by a computing system.
- Create opportunities for members of the organization to learn the principles and limitations of computer systems.

Compliance with the code

As an ACM member, I will

- Uphold and promote the principles of this code.
- Treat violations of this code as inconsistent with membership in the ACM.

FIG. 43.2

Association for Computer Machinery Code of Ethics and Professionals. (From <http://www.acm.org/about/code-of-ethics>, accessed 31 March, 2011. With permission.)

working at the leading edge of technology place network security high on the priority scale as the network provides both the access and the security required for continued operations. They understand that building a security culture is important to the organization's survival in a highly competitive marketplace. For a security culture to be evident, management must initiate effective security practices and fully support the perpetuation of these practices. A security culture promotes security aware attitudes, values, and employee behaviors in order to protect the organization's physical and logical assets.

A security culture is a sociotechnical aspect of network security. The human element is predominantly the weakest link in an organization's security; however, a secure infrastructure will minimize the risk of insider abuse as well as attacks from the outside. An effective security culture at the

organizational level will be reflected in secure practices at the network level and will be reinforced by security policies and procedures in administering the network. If senior executives are seen to be security conscious, then employees will adopt a similar set of values.

A security culture is inextricably linked to ownership of the wellbeing of the organization and its core networks. If employees feel a loyalty to the organization and their goals are aligned with those of the organization, then a security culture is much easier to build. Some examples of the evidence of a security culture would be questioning unfamiliar people in the area usually occupied only by employees, or the intolerance of colleagues contravening the policies and procedures by downloading nonapproved materials or executing questionable software.

NETWORK SECURITY MANAGEMENT

Management of network security is a balance between resources, accessibility, and security. The implementation of security measures tends to limit accessibility and usability. The higher the level of security, the less accessibility users have. Each organization must balance the needs of accessibility with security and its utilization of their resources. One organization will have different security requirements to another. The level of security required for a network depends on the type of network and the facilities that network is required to offer. For example, the security on a network connecting resources dealing with research and development for defense applications will be greater than a network providing information to the public on government services. Complex networks can be more difficult to secure, depending on the topology, level of traffic, and sensitivity of the data stored and transmitted.

At the management level, a corporate security approach is needed; involving an integrated risk analysis, information classification, information ownership, incident handling, security education, and network contingency planning. Commencing at the grass roots level, employees must be aware of security, and understand what security measures are in place and why. They must also understand how security assists an organization in reaching its goals and objectives. If network security does not assist an organization to achieve its objectives, then security measures should be reconsidered. More security means less accessibility, and users need to be able to do their jobs with as little resistance as possible. Network security should also be transparent to the user.

Defense in depth is the use of concentric layers of security around an asset for protection. In history we find that castles were built with high, strong walls, and commonly surrounded by a moat of water with a single point of entry—the drawbridge. This is a physical implementation of the defense in depth principle. This principle is also applied to network security via the use of a combination of security techniques to protect the network, such as antivirus software, firewall, and intrusion detection in addition to encryption of the core data. Defense in depth also works with a combination of security factors that involve people, technology, and procedures, where solutions incorporate more than just technological hardware and software.

In general, network security management embraces activities in the following areas:

- Security policies
- Network risk analysis and risk management
- Information classification and enforcement
- Secure personnel practices
- Planning and budgeting
- Network quality assurance
- Physical security
- Contingency planning
- Responsibility and accountability

- Network asset ownership and accessibility
- Custodianship of network assets
- Incident response

International Standards for Information Security Management

There are international standards for information security management, the current version being the ISO/IEC 27000 [7] series commonly referred to as ISO 27k. This standard originated from British Standard 7799 and the Australian Standard AS17799. Although the ISO 27k series focuses on information security management, it provides the framework within which the network security management standard is positioned. The entire set of ISO 27k standards provides a comprehensive coverage of security management at all organizational levels.

Computer networks are implemented to assist an organization to achieve its goals and mission, and effective network security management will need to be adapted to the specific organizational setting. The ISO 27k standard provides guidance in establishing and managing security and consists of the following suite of detailed standards to assist management:

- ISO/IEC 27000—the overview to the 27k standard set and includes the vocabulary used.
- ISO/IEC 27001—the Information Security Management System requirement standard for organizational certification.
- ISO/IEC 27002—the Code of Practice for Information Security Management including the control objectives and good practice security controls.
- ISO/IEC 27003—the Implementation Guide for the certification in 27001.
- ISO/IEC 27004—the Information Security Management Measurement standard consisting of metrics to improve the effectiveness of an Information Systems Management System.
- ISO/IEC 27005—the Information Security Risk Management standard consisting of guidelines and a management approach for information security risk.
- ISO/IEC 27006—the guide to the Certification Process for accredited certification bodies.
- ISO/IEC 27007—the guidelines for Information Security Management Systems for accreditation as per 27001 and 27002 for use by accredited certification bodies, internal auditors, external and third party auditors, and others auditing Information Security Management Systems.
- ISO/IEC 27008—the guide for Auditing Information Security Management Systems controls through a risk-based approach.
- ISO/IEC 27010—the guide for Information Security Management for sector-to-sector communications, including guidelines for sharing information on

security risks, controls, and incidents between organizations in the same sectors and across different sectors with particular application to critical infrastructure.

- ISO/IEC 27011—the Information Security Management guide for Telecommunications organizations, based on the ITU X.1051.
- ISO/IEC 27013—the guide for integrated implementation of ISO/IEC 2000-1 (ITIL) and the ISO/IEC 27001.
- ISO/IEC 27014—the Information Security Governance guide, providing information on risk management, management controls, compliance, and assurance activities plus security accountability and responsibility issues.
- ISO/IEC 27015—the Information Security Management guide for financial services organizations, providing guidelines for financial organizations to meet baseline information security management requirements.
- ISO/IEC 27031—the Information and Communication Technology (ICT) focused standard on business continuity, including a set of processes and methods for organizations to improve ICT readiness to ensure business continuity and a means of measuring an organization's ability to survive a disaster.
- ISO/IEC 27032—the guide for cyber-security, including the components of cyberspace, the threats against the security of cyberspace, guidelines for stakeholders, and cyberspace security controls.
- ISO/IEC 27033—the guide for IT network security including the ISO/IEC 18028 standard. This provides guidance on the security of the management, operation, and use of information systems networks. A more detailed discussion of this standard follows.
- ISO/IEC 27034—the Applications Security guide, providing information security guidance for the specification, design, programming, procuring, implementing, and using application systems.
- ISO/IEC 27035—the Security Incident Management guide based on the ISO TR 18044 standard and also incorporating a common classification system.
- ISO/IEC 27036—the Security of Outsourcing guide, providing guidance on the evaluation and mitigation of security risks involved in outsourcing.
- ISO/IEC 27037—the Digital Evidence guide. This includes guidelines for the identification, collection, and preservation of digital evidence.
- ISO/IEC 27799—the Health Sector Information Security Management System implementation guide, based on ISO/IEC 27002. This provides detailed controls for managing health information security to ensure availability, confidentiality, and integrity.

Many of these standards are under revision or still under development. ISO/IEC 27033 is currently under revision and focuses on IT network security and provides guidance for the security management, operations, and use of networked information systems. The information given in this standard

is able to be adapted to meet an organization's specific requirements to secure their ICT networks. ISO/IEC 27033 encompasses the following areas:

- *Network security overview and concepts.* This section provides an overview of the concepts and terminology used in network security and provides management guidance on identifying and analyzing network risks and defining network security requirements for the organization in question. It also gives advice on control aspects of network topologies, and maps all the parts of the standard.
- *Guidelines for the design and implementation of network security.* These guidelines outline how an organization can achieve quality network technical security architectures, designs, and implementations to ensure a level of network security that is appropriate to their particular business situation and environment.
- *Reference networking scenarios.* Identifies the specific risks, design techniques, and control issues related to typical network scenarios.
- *Secure information flow.* Threats, design techniques, and control issues relating to securing communications between networks using security gateways.
- *Securing Virtual Private Networks (VPNs).* Focuses on the threats, design techniques, and control issues for securing VPN connections.
- *IP convergence.* Aims to define the specific tasks, design techniques, and control issues for securing networks converging data, voice, and video.
- *Secure wireless networks.* This section covers the risks, design techniques and control issues associated with securing wireless and radio networks.

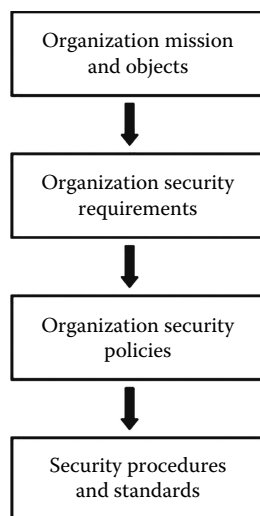
This network security standard provides a comprehensive set of international guidelines for best practice in the ongoing management of network security.

Network Security Policy

The corporate security policy must support organizational objectives and integrate with organizational strategies. The corporate level security policy is the umbrella for the array of security policies that an organization needs to implement. Security policies must be written, be generic in nature (not specifying hardware and software details that may become outdated), be succinct, and be distributed to all users. It is advisable to gain each user's signature to verify that they have read and understood the key security policies. It is important that security policies are enforced to ensure continued adherence and awareness of security requirements. Each policy should state the action and penalties for noncompliance.

Policies are converted into procedures and standards that ensure compliance of the policy as illustrated in [Figure 43.3](#).

The organization needs an array of specific security policies that enforce the overall security policy. Effective network security policies form an integral part of managing the

**FIG. 43.3**

The linking of security policies and procedures.

organization's computing environment and the breadth of security policies should include policies for:

- Acceptable use of systems and networks
- Firewall and IDS/IPS implementation and management
- Authentication devices such as smart cards, tokens, or biometric devices
- Password management and encryption
- Physical security requirements relating to networks
- User access to systems including alternate methods of accessing the Internet
- Virus minimization requirements
- Maintenance of confidentiality via nondisclosure agreements
- Encryption of sensitive data in storage and in transit
- Acceptable and unacceptable user Internet usage or access to sites
- Operating and application software standards
- Responses to network intrusions
- Data backup and recovery
- Powering-up and powering-down the network
- Remote access
- Data classification levels and handling of sensitive data
- Network contingency planning

SysAdmin, Audit, Network, Security (SANS) is a well-known information security training and certification organization. Its website has an excellent array of example information security policies that may be freely downloaded and utilized (<http://www.sans.org/resources/policies/>). However, a given policy will not suit all situations and each organization must develop policies that meet their own requirements to fit their specific environment.

Corporate level security policies need to be in place to ensure that all the networks in an organization's computing

environment support the high-level mission and objectives as well as being secured to a standard level. Large organizations will usually have an array of networks with each network designed for a specific purpose and the security on each network will depend on its purpose. Security measures placed on the network should consider the type of user, the data stored and accessed, and the tasks that network will carry out.

Information Classification and Ownership

The data stored on ICT networks is not owned by the IT Department, it is owned by the business owner in the department that initiates and has responsibility for that information. The IT Department is purely the custodian of that data. All data files and databases processed and stored on networks must have stated owners who declare the level of security required for that data and rules for accessibility, modification, and use. The ICT Department ensures that the applications that use that data uphold the security requirements stated by the information owner.

Organizations need to devise an information classification in order to ensure that sensitive information is protected in the activities of input, processing, storage, and output. An information classification should be a sociotechnical program to classify the organization's different types of information and devise the minimum necessary activities to protect each level of classification. In some industries, classifying information is performed to meet regulatory requirements, while in others, it is used as a governance measure to protect information at all stages of its life cycle.

If an organization does classify its information, then there must be processes to handle the reclassification of data and equipment related to sensitive projects over time. Sensitivity of information is usually determined by a series of factors, but the most prominent is time. Sensitive data usually relates to an event in time, for example, the release of a new product, or research and development toward a set deliverable. Classification measures provide security, if the event is in the future, and possibly current, but once the event has passed then the classification level may need to be altered as the sensitivity of the data, product, or equipment changes.

Information has different values to different parties. Parties interested in information include decision makers within the organization, directors, joint partners, customers, suppliers, finance providers, competitors, and so on. Each party uses the information in a different way, and the loss or misuse of information, or unauthorized access and modification of information can impact an organization's survival in a competitive marketplace, or a nation/state's security. While classifying data we need to be cognizant of why we are protecting it, and from whom.

A four-level classification system commonly used by commercial organizations consist of the following:

Level 1—Highly sensitive: This information is for access by named individuals only. Its release, loss, or misuse could

seriously damage the organization. This is top secret information. This information should be encrypted in storage and communications, and users accessing this data or equipment require authentication, identification, and verification. One-time passwords and biometric and/or smartcard authentication should be considered for access to highly sensitive information and equipment.

Level 2—*Sensitive*: This information is restricted to a well defined group of people, such as a Department or Project Group, or relates to a subject matter that is high in value. Sensitive information requires authentication and identification, and secure access by strong user ID and passwords is recommended. Biometric or smartcard authentication may also be used.

Level 3—*Company in confidence*: Restrictions apply at this level to keep the information or equipment within the organization. Strong user IDs and passwords should be enforced. Smartcard authentication may also apply, depending on the situation.

Level 4—*Public or unrestricted*: This information is freely available and does not require User ID or password to access.

Labels clearly indicating sensitivity levels must be posted on documents, data, and devices. Information assets can be labeled using header or footer records on electronic files; on-screen labels displaying the classification level plus any associated warnings, encrypted, and transmission of classified data can be labeled as well as controlled by secure administrative interfaces.

The handling of confidential information should also be governed by strict procedures. Depending on its classification level, information must have corresponding procedures for access, copying, transmission, backup, printing, physical delivery, and electronic and hardcopy storage. Procedures for the destruction of confidential information assets must ensure that the information is disposed of via secure mechanisms that render it nonretrievable.

The classification level is assigned by the information or equipment owner. Any reclassification or declassification should also be initiated by the owner. Policies and procedures for any change in classification level should be clearly specified. Requirements for the handling and marking of each classification level should also be stated in policies, procedures, and job descriptions. Systems to manage data and equipment at higher levels of sensitivity should be in place, with management procedures defined and accountability assigned. Any release, loss, or misuse of confidential information or equipment must be able to be tracked to its source.

Secure Personnel Practices

Secure procedures and practices around the hiring and firing of key network and IT personnel are foremost in the protection of corporate information and assets. With the current high rates of turnover for IT employees and the use

of outsourcing partners for IT security and support, risks to an organization's information assets are increasing. Many IT personnel have access rights that exceed their roles, with prior rights being rescinded when the individual moves to a new role.

Hiring New Staff At the hiring stage, applicants should be screened thoroughly and references checked in detail. Claimed skills can be checked by requesting the applicant to complete a test requiring tasks that relate to essential parts of the position. Upon hiring, a nondisclosure agreement as well as an agreement on employment terms and conditions, including intellectual property and terms forbidding the establishment of a competing business, or employment with a competing organization in any form, should be signed.

Ongoing Employment A formal job description should be provided, referring to policies and procedures required by the position. Performance evaluation criteria need to be established at the time of appointment to the position and regular evaluation of performance should be carried out. The performance evaluation meeting presents an opportunity to not only discuss the employee's progress but also reinforce awareness of security policies and procedures and acceptable behavior on the network. Negative motivation is a strong contributor to insider abuse, and regular performance progress meetings enable employers and employees to discuss performance expectations and management.

Separation of duties is a recommended practice where tasks fall into key areas of network management. More than one person should be responsible for crucial tasks so that these tasks are shared, making it less likely for abuse due to the need for collaboration. The granting of privileged access and knowledge regarding network security mechanisms requires careful supervision. The escalation of security concerns to a senior executive where cases involve that line of management is also required.

Termination When employees leave the organization, either through resignation or termination, there are several key issues that need to be addressed. All access rights, both logical and physical, should be removed at the time it becomes known that the individual is leaving. This will minimize the risk of devious and fraudulent activity (copying files, loading viruses and Trojans, etc.). It is important to terminate access to all networks, IT systems, and ICT facilities. Where the individual holds a position of trust, it is recommended that an audit of their activities and workstation be performed before departure. Individuals dealing with sensitive information are commonly escorted to their desks to gather personal belongings and then to the door by security officers. All company equipment must be returned including ID cards, smart cards, laptops, USB devices, phones, etc.

It is advisable to hold an exit interview with the terminated employee. This provides the individual with an opportunity

to voice grievances, thus reducing motivation for abuse. It is also an opportunity for the organization to gather information on activities in the workplace that may not be known. The departing employee can be made aware of any restrictions placed upon them by prior agreements signed, covering areas such as nondisclosure and restrictions of establishing a competitive business.

Additional Security Management Measures

At an operational level, network security measures should incorporate safeguards on physical network assets and the physical environment, logical security measures to protect data and software, communications security, security measures within the system development process, and sound change controls. Written policies, procedures, and standards need to embrace these operational measures. In addition, regular security reviews and audits need to be carried out on the network environment to ensure that security measures are operating at the desired levels of performance.

RISK ANALYSIS

This section discusses an approach to analyzing risks in a networked environment. Before we embark on a detailed discussion of the risk management process, it is important to understand the difference between threats, risks, and vulnerabilities with relation to computer networks. A *threat* is something that has the capacity to cause harm or damage to the network or organization via the network, for example, virus, unauthorized access, phishing, or industrial espionage. For more details on specific threats to networks, see Chapters 29 through 31 and 35. A *risk* is the possibility that a threat may actually occur and this is often measured by a level of risk exposure, which will be discussed shortly. A vulnerability is a weakness that exposes the network and enables a threat to actually cause harm, for example, software bugs, unpatched software, and theft of hardware. It should be noted that threats include both intentional and unintentional events such as human errors.

The process of network risk analysis determines the threats that face a networked system, studies the likelihood of damage or loss, and the consequences of the occurrence of threats. Security measures can then be investigated and evaluated to address these threats. Threats to networked systems are discussed in detail in Chapter 35; however, some of the prominent threats include

- Viruses and worms
- Trojans
- Spam
- Phishing
- Packet sniffers
- Port scanners
- Maliciously coded websites

- Spyware
- Shared computers
- Hardware loss
- Residual data fragments
- Botnets
- DoS attacks
- Password stealing
- Identity theft
- Data loss

Although the two terms are often used interchangeably, risk management is not the same as risk analysis. Risk analysis is the process of investigating and assessing risks, whereas risk management is the overall process to manage risk to an acceptable level. Risk management includes assessing threats, determining risk exposure, implementing controls, and measuring the effectiveness of selected countermeasures. Risk analysis is only one process within risk management. The process of risk analysis and its relationship to other security management functions can be seen in Figure 43.4.

Network risk analysis and risk management are essential tasks in order to ensure that the networked environment remains secure. Analyzing the risks inherent in networked environments forms a key part of the overall computer risk management process. As networks provide the infrastructure, applications, and data storage for an organization, the analysis of risk is a core process in the secure management of these integrated environments.

There are many models for ICT risk management with different levels of detail; however, the core activities are the same for all. The IEEE Risk Management model [4] (IEEE Standard 16085:2006) comprises six steps:

1. Planning and implementing risk management
2. Managing the project risk profile
3. Performing risk analysis

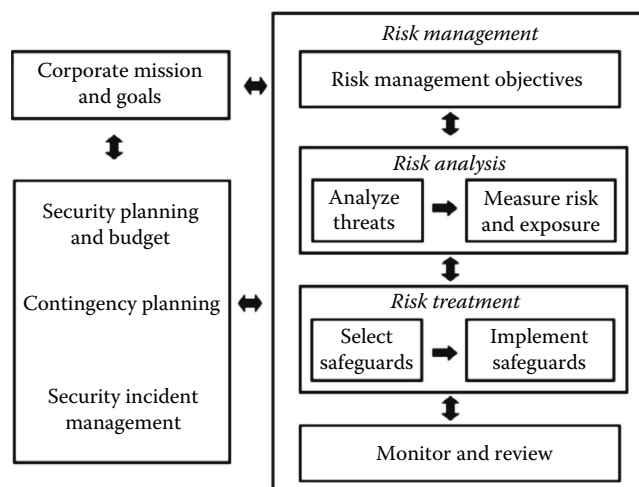


FIG. 43.4

The risk management process.

4. Performing risk treatment
5. Performing risk monitoring
6. Evaluating the risk management process

ISO 31000:2009 Risk Management Principles and Guidelines [6] standard supports the establishment of a risk management framework in a loop comprising

1. Design the risk framework
2. Implement the risk framework
3. Monitor and review the risk framework
4. Continual improvement of the risk framework

The risk framework is then used to establish the context of risk management and process risk assessment through risk identification, risk analysis, risk evaluation, and risk treatment. This process is carried out by integrating communication and consultation and monitoring and reviewing. The ISO standard defines risk as the effect of uncertainty on objectives, thus permitting its application to different types of risk management across the organization.

Information Systems Audit and Control Association has also developed the RISK IT framework, which is based on the COBIT model for governance and control of IT environments. Incorporating the principles from ISO31000, Risk IT comprises the following processes [5]:

1. Risk governance;
 - a. Establish and maintain a common risk view
 - b. Integrate with ERM (enterprise resource management)
 - c. Make risk-aware business decision
2. Risk evaluation
 - a. Collect data
 - b. Analyze data
 - c. Maintain risk profile
3. Risk response
 - a. Articulate risk
 - b. Manage risk
 - c. React to events

Other risk management models and standards also exist; however, for simplicity, the risk management process comprises the following general activities (Figure 43.4):

- Determining security risk objectives from the organization's mission and goals
- Identifying and analyzing threats to all parts of the ICT environment
- Determining the organization's vulnerabilities, the likelihood and impact of threats occurring, and the risk exposure
- Determining security solutions that are cost-effective and appropriate for the given ICT environment and any residual risk

- Implementing approved and appropriate solutions
- Monitoring threat levels and risks, as well as ensuring safeguards continue to meet security requirements

Determining Risk Management Objectives

Security is implemented to aid the organization to minimize the level of risk it needs whilst achieving its goals. If a security measure does not assist an organization to achieve its goals, then the security measure should not be implemented. Be cognizant that security must balance with the level of risk and the security required, and users will become frustrated where security is too strict for them to carry out their jobs and efficiently meet their employment requirements. The level of risk exposure to a given threat should determine the level of safeguard needed.

Analyze Threats and Vulnerabilities

Threats that pose potential danger to an organization's networked environment need to be identified and then analyzed to determine the likelihood of occurrence and their potential impact. A review of security will also provide indications of vulnerabilities in the ICT environment, and this will provide input into the analysis of the threats and their likelihood of occurrence. A review of current security measures, procedures, and threats relating to information and information assets within an organization aims to determine the existing security state as well as locate weaknesses and security recommendations.

Threats that affect networks can emanate from both human and technical sources. Some example threats include

- Human errors
- Rogue code including viruses, worms, and Trojans
- Phishing
- Denial of service attacks
- Unauthorized access
- Equipment failure
- Equipment damage
- Design faults
- Improper modifications
- Loss of skilled staff
- Lack of documentation
- Lack of technical training
- Careless disposal of information
- Destruction of data
- Theft of software, data, or equipment

Threats to a network will be directly associated with physical, logical, and human aspects of that particular network and specific threats to a given networked environments should be identified by the organization. The following examples are based on the Australian Defense Security Directorate's information security manual [3]:

- An attacker targets an unmanaged section of a network, compromising the confidentiality, integrity, and availability of the data.
- A system administrator makes an undocumented change to the network that exposes internal systems, inadvertently allowing unauthorized access to information.
- An attacker makes a change to the configuration of communication equipment in order to access information on the network.
- A systems administrator makes a change to the network without understanding the impact to other parts of the network inadvertently allowing unauthorized access to information, affecting the integrity of network data or denying network access to authorized systems users.
- An attacker intercepts traffic being communicated over the network, allowing them unauthorized access to information.
- An attacker intercepts traffic relating to the management of the network, subsequently using this information to develop more focused attacks.
- An attacker with access to one part of a network is able to propagate this access across other sections of the network that contain information or data of a higher security classification.

Measuring the likelihood of a threat occurrence can be carried out either as a quantitative measure as the number of occurrences per annum or as a nominal or ordinal rating, for example, 1–5 where 1 is very low probability of occurrence and 5 very high. The interval between numbers or codes assigned is not equal, so an explanation of each ranking must be clearly defined. Table 43.1 illustrates an example threat likelihood table for a seven-level rating approach.

An audit of current network security will detail areas of vulnerability. These could be the result of new threats, changes to equipment or network management applications,

installation of new or replacement network equipment, changes in staffing key areas of network administration, and the like. The security review or audit is normally carried out by the internal audit function within large organizations or a team of consultants from outside the organization.

A more common approach to testing the security of the network is to hire specialists to attempt to break into the network using hacking tools and techniques. Such experts were previously termed tiger teams, now referred to as penetration testers. Penetration testers simulate actions of attackers in order to identify vulnerabilities in the organization's ICT environment. It is recommended that rules of behavior are established prior to the penetration testing to ensure minimal impact on the operational environment. Many penetration tests result in unexpected outcomes raising the need for agreed incident response procedures to be followed in case of such events. Organizations wishing to use penetration testers to audit their own networks should consult with legal advisors to ensure that legalities are handled regarding criminal acts as well as liability for loss or damage caused by the testing. It is highly advisable to establish an agreement between the parties to ensure that there is a common understanding of the scope and constraints in addition to indemnity for loss or damages.

Measure Impact and Risk Exposure

The occurrence of each threat will have a different impact on the organization and these impacts will need to be determined in order to understand the importance of the threat when choosing solution investment strategies. For example, an attack involving unauthorized access and theft of valuable intellectual property for sale to a competitor will have different implications for the organization to that of a fire in the server room. The impact of a threat could result in network downtime resulting in loss of income for the organization as well as productivity, replacement of hardware, software, and/or data, or additional staffing costs for recovering systems and data. It may be difficult to estimate values for the more intangible impacts such as employee morale or loss of market share.

In some circumstances, the losses may not be easily estimated in raw figures. In these circumstances, the impact of threats can be rated by levels in a similar approach to grouping threats. Symantec use a three-level ranking: low, medium, and high severity. Table 43.2 illustrates an approach to classifying the impact of threats using six levels.

Some threats will mean that the impact may change over time. For example, manual procedures can usually holdout for short periods, depending on the reliance on the systems in question. For example, the impact of network downtime via a denial of service attack on mission critical systems becomes more critical as the downtime period extends.

Estimates of potential losses based on the impact of a threat occurring can assist in determining a level of risk exposure an organization may suffer. The risk exposure calculation is used as a guide to assist decision makers. It indicates the potential extent of exposure each threat may have

TABLE 43.1

An Example Threat Rating Approach

Rating	Description
Minor	Unlikely to occur
Very low	Likely to occur once every 2 or 3 years
Low	Likely to occur once every year
Medium	Likely to occur once every 6 months
High	Likely to occur once every month
Very high	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

Source: Excerpt from CERT, Targeted Cyber intrusion, mitigation strategies matrix, Computer Emergency Response Team and Defence Signals Disectorate, Australian Government, 2009. http://www.cert.gov.au/www/cert.nsf/Page/Alerts_and_Advisories

TABLE 43.2*An Example Impact Rating Approach*

<i>Impact Rating</i>	<i>Description</i>
Negligible	Almost no impact
Minor	Some minor effect on operations
Significant	Loss or damage to key information assets, some negative effects on service or product provision
Damaging	Loss of information or services that could damage the organization's reputation or information integrity, loss of confidence, significant expenditure
Serious	Severe implications, extended system outage, compromise of large amounts of data
Grave	Unlikely to recover, cause permanent closure

on the organization. A simple calculation for risk exposure can be obtained from the following formula:

$$RE = PO \times LO$$

where RE = Risk exposure (\$ Loss p/a)

PO = Number of probable occurrences p/a

LO = \$ Loss per occurrence

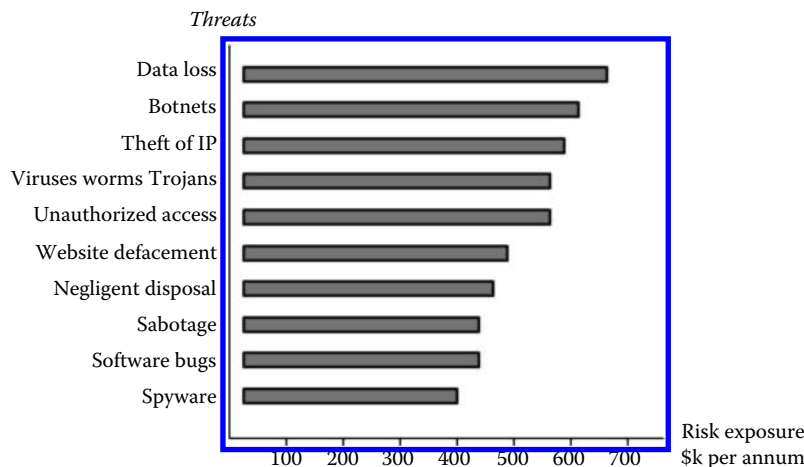
The first step is to determine an approximate cost for each occurrence of this particular risk. This could comprise the replacement cost of the asset (e.g., hardware, software), costs of restoring the network to good working order, additional staffing costs to recover data, implementing countermeasures to block recurrence, and the like. This figure is the *\$ Loss per occurrence*. The second step is to estimate the number of occurrences that are likely to occur in a 1 year period. It can be obtained from historical data detailing past occurrences or estimates based on log entries. If it is a green-fields situation, an indication may be obtained based on data from similar organizations in the same industry. This figure is the *number of probable occurrences* per year. The *risk exposure* expected for a year would then be the number of probable occurrences per year, multiplied by the \$ loss per occurrence.

The risk exposure for different risks can then be compared to determine the risks that have the potential to cause the greatest losses to the organization. Figure 43.5 illustrates the comparative risk exposure for a selection of network security risks calculated for an example organization. This bar chart shows \$k risk exposure per annum on the Y-axis and the type of risk along the X-axis of the bar chart. This type of comparison provides guidance to the organization for decisions regarding financial investment in countermeasures.

Select and Implement Safeguards and Manage Residual Risk

After identifying those threats to be addressed with security measures, a scan of available options is undertaken to identify potential safeguards. Safeguards can be procedures, applications, and/or devices. Potential safeguards are evaluated to determine the most appropriate and cost-effective solutions and any residual risk not addressed by the solution.

In many cases, the solution to security threats can be addressed by simple mitigation strategies. The Cyber Security Operations Center listed the top 35 mitigation strategies together with the ranking of the effectiveness and costs of each. The mitigation strategies with effectiveness ranked to be excellent or good are listed in [Table 43.3](#).

**FIG. 43.5**

Comparative bar chart showing risk exposure for threats.

TABLE 43.3*Effectiveness and Costs of Mitigation Strategies (Excerpt from the Matrix Compiled by CERT 2009)*

<i>Ranking</i>	<i>Mitigation Strategy</i>	<i>Security Effectiveness</i>	<i>Upfront Cost</i>	<i>Maintenance Cost</i>
1	Patch the operating system	Excellent	Medium	Medium
2	Patch third party applications	Excellent	High	Medium
3	Minimize administrative privileges	Excellent	Medium	Low
4	Application white listing	Excellent	High	Medium
5	Host-based intrusion detection/prevention	Excellent	Medium	Medium
6	Workstation conversion/sanitization of Microsoft Office files	Excellent	Medium	Low
7	White-listed e-mail content filtering	Excellent	High	Medium
8	Gateway with split DNS server, e-mail server, password authenticated web proxy and firewall preventing workstations directly accessing the Internet	Good	Low	Low
9	Data execution prevention	Good	Low	Low
10	Antivirus software with up-to-date signatures and heuristic detection capabilities	Good	Low	Low
11	Sender policy framework to help block incoming spoofed emails	Good	Low	Low
12	Audit reconnaissance tool usage	Good	Medium	Low
13	Restrict access to NetBIOS	Good	Medium	Low
14	Application based workstation firewall to control incoming traffic	Good	Medium	Medium
15	Network segmentation and segregation	Good	High	Medium
16	Centralized logging and regular log analysis	Good	High	High
17	Disable unrequired operating system functionality	Good	Medium	Low
18	Application security configuration hardening	Good	Medium	Medium
19	Application-based workstation firewall to control outgoing traffic	Good	Medium	Medium
20	Web domain white listing for domains using HTTPS/SSL encryption	Good	Medium	Medium
21	Web content filtering	Good	Medium	Medium
22	Two factor authentication	Good	Medium	Medium
23	Removable media control	Good	High	Medium
24	Web domain white listing for all domains	Good	High	Medium

National Institute of Standards and Technology in 2008 [8] recommends the following set of preventative measures to ensure minimization of network intrusions:

- Configure firewalls and other security controls to prevent the use of applications that violate the organization's security policies.
- Configure the organization's e-mail servers to deny unauthorized mail relaying to limit spam originating from the network.
- Implement spam filtering on all e-mail servers.
- Implement URL filtering to prevent access to inappropriate or forbidden websites by the use of proxy servers.
- Limit outbound connections that use encrypted protocols such as SSH, HTTPS, and IPSec. These protocols limit the organization's ability to monitor traffic content.

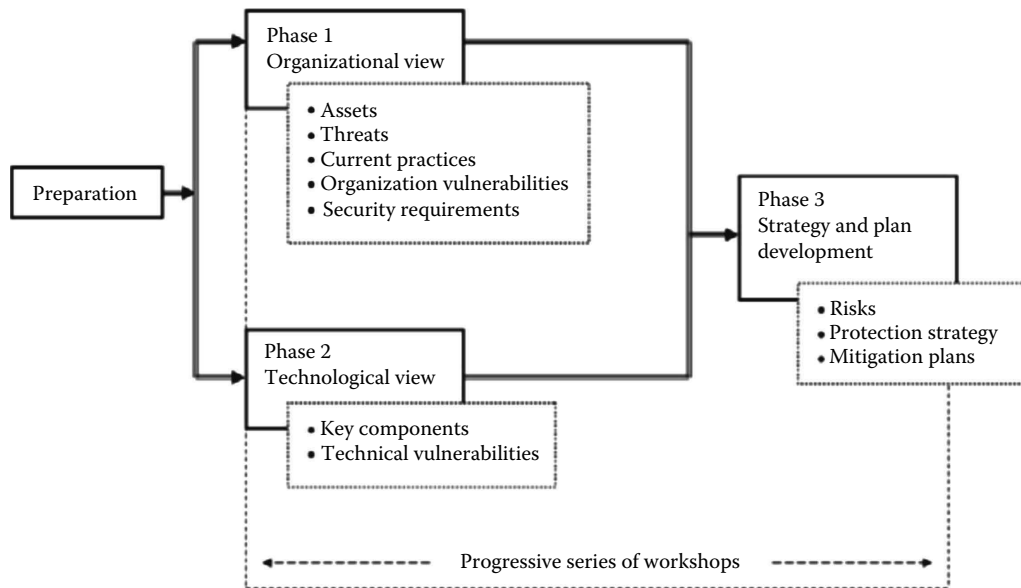
The process of implementing safeguards involves the obtaining or developing of the chosen security measures, physical installation and testing of these, and training users in their operation. Information regarding security measures should then be defined in procedures and included

in job descriptions of those assigned responsibility for the management and use of these measures. Knowledge of safeguards must be limited on a need-to-know basis. For example, an organization has implemented a solution to encrypted user activity logs and stored these in a separate area of the network. Details of this facility should only be made known to those who are directly responsible for the control of this facility or those responsible for the checking of these logs.

Monitor Safeguards, Threat Levels, and Risks

Safeguards need to be regularly reviewed to ensure that they are operating and performing effectively and provide the desired level of protection. The appropriateness of safeguards and the operation costs should also be reviewed. A review should also take place on changes to system platforms and key applications, or when new threats appear.

CERT at Carnegie Mellon University developed a risk analysis tool named OCTAVE [1] (operationally critical threat, asset, and vulnerability evaluation). The OCTAVE process is illustrated in Figure 43.6. OCTAVE uses a three-phased approach as follows (<http://www.cert.org/octave/methodintro.html>):

**FIG. 43.6**

*The OCTAVE® approach. (From Caralli, R.A. et al., *Introducing OCTAVE Allegro: Improving the information security assessment process*, Technical Report CMU/SEI-007-TR-012, Carnegie Mellon University, Pittsburgh, PA, 2007.)*

- *Phase 1—Build asset-based threat profiles:* This phase investigates key area of the organization to identify important information assets, threats to those assets, their security requirements, and current protective practices, in addition to weaknesses in policies and practice. The security requirements for each asset are based on the standard confidentiality, integrity, or availability model.
- *Phase 2—Identify infrastructure vulnerabilities:* This phase investigates network paths, and weaknesses and vulnerabilities in the information technology infrastructure are identified.
- *Phase 3—Develop security strategy and plans:* The findings from phases 1 and 2 are analyzed with relation to their risks and impact to the organization's mission. In the final stages, risk analysis scenarios are used to create risk profiles, and protection strategies are developed and mitigation plans are established for high-priority tasks.

The OCTAVE process is carried out by a small team involving members from both mission-critical as well as IT areas who are responsible for managing the process and analyzing the information. OCTAVE uses two types of workshops. The information-gathering workshops catalog and analyze information and determine current protection mechanisms and vulnerabilities. The consolidation and analysis workshops produce key operational components of the information infrastructure, risks, protection strategies, and mitigation plans to minimize risk to critical assets. The catalogs of information it produces are:

- *Catalog of practices*—good strategic and operational security practices
- *Threat profile*—range of threats to consider
- *Catalog of vulnerabilities*—compilation of vulnerabilities relating to different platforms and applications

Benchmarking against internationally recognized catalogs of threats and best practices is advisable for every organization, ICT activity. CERT [2] recommends benchmarking the threats from the OCTAVE process against a common directory such as common vulnerabilities and exposures (CVE), BugTraq, or the SANS top 20. CVE is an international dictionary of publicly released information security exposures and vulnerabilities. CVE is managed by the MITRE Corporation and can be found at <http://cve.mitre.org>. BugTraq is an electronic mailing list distributing details of vulnerabilities and exploitations and methods of addressing these. It is hosted by Security Focus at <http://www.securityfocus.com/archive>. The SANS Top 20 is the top 20 vulnerabilities and security risks identified via data collected from more than 9 million computers and analyzed by the Internet Storm Center and specialist SANS personnel. Details are available at <http://www.sans.org/top-cyber-security-risks/>. These internationally recognized directories provide an informed and up-to-date source of detailed threats and vulnerabilities.

SECURITY INCIDENT HANDLING

A security incident is an event that is a violation or imminent threat of violation of some parts of the computer security

policy. Security incidents commonly involve unauthorized access, unauthorized activities, and/or denial of authorized access to systems or information. It is recommended that organizations develop, implement, and manage procedures and tools to detect potential security incidents. Basic activities of all organizations should include implementing safeguards against all types of malicious code, strategies to detect intrusions, regular system audits, and vulnerability analysis. A regular risk analysis will provide an indication of the amount of resources to allocate to the detection and prevention of security incidents.

The first step an organization needs to take is to establish a definition of the term “incident” the services an incident response team should provide, the team structure and models to provide those services and then implement one or more incident response teams [8].

Many security incidents are identified by employees working with the systems; hence, it is important that these individuals are well trained to recognize the characteristics of common exploits and means of mitigating these. Provided automated tools are kept updated with new vulnerabilities and abuse signatures, they will perform the security functions for which they were designed; however, these tools quickly become outdated resulting in reduced effectiveness.

The most common tools used in security incident detection include the following:

- *Intrusion detection systems*—host or network that monitor and analyze network activities using a database of known attack signatures
- *Intrusion prevention systems*—operate in conjunction with an IDS and act on the detection of known attack signatures
- *Anomaly detection systems*—identify activities that do not conform to normal patterns of system activity or usage
- *Log analysis*—analyzing event logs to identify abnormal activity using pattern recognition
- *System integrity alerts*—detect unauthorized changes to critical systems, files, directories, etc., and alert the system administrator

It is important that an organization has a planned, well-structured approach to incident handling and response. Each organization will need to develop an approach that is appropriate to its goals, activities, and size. The process of security incident management is organized as follows [9]:

1. *Preparation*: Including setting objectives for the incident response function, establishing rules for response to attackers and procedures for bringing in law enforcement, carrying out risk analysis, and actively monitoring the network. Training the incident response team is also included in this stage.

2. *Notification*: Awareness of a potential intrusion from the firewall, IDS, or a network administrator who detects abnormal activity. Documentation of abnormal events and their effect on the network is then performed. Investigation of the spread of infection or extent of damage is also performed and registered.
3. *Response*: Procedures for permitted actions in response to attacks should be clearly detailed together with decision points and procedures for escalation. Procedures need to provide guidance for actions to limit damage, protect company data, recover lost data, and/or maintain client confidence. Such procedures will ensure a response that can be initiated within a minimum time frame, thus limiting further damage. Prior risk analysis performed by the organization can provide guidance for the importance of the resulting action regarding critical asset protection. Incident response procedures need to detail what needs to be reported, who needs to know, and how quickly it should be reported.
4. *Countermeasures*: Containment is the first action to prevent further damage to information assets and equipment. Ideally, the problem needs to be contained within a well-defined section of the network where perimeter security measures can limit its movement and damage to other parts of the network. Common actions to contain an intrusion include shutting down the affected system, disabling user and group accounts, disabling services that were exploited, and making images or backups of affected systems to protect the originals as evidence. Eradication is the task of removing any files or applications resulting from the intrusion, and these can include malicious code, registry keys, unnecessary executable files, viruses, worms, or files created by worms.
5. *Recovery*: Actions to recover the network back to normal operations include monitoring restored devices and applications to ensure the network is operating correctly and no undetected vulnerabilities remain.
6. *Follow-up*: Documenting the incident detection and every action in the response is necessary to keep a record of intrusions for reference in the future. Details of actions taken during the response and the results should also be noted, giving guidance for personnel involved in similar incidents in the future. Much of this documentation will be needed to rebuild the scenario and also provide evidence if legal action is to be taken against an attacker. All documentation needs to be handled as if it were evidence and protected appropriately. Security policies and procedures should be reevaluated and any change to these should also be detailed in the incident documentation.

CONCLUSIONS

Security of the network relies on effective proactive management activities, carried out in timely manner to ensure the organization's information assets and computer equipment remains protected. The implementation of several layers of protective measures between the attacker and the targeted asset will reduce security incidents. Security aware employees are the organization's first line of defense, closely supported by automated applications, and tools to defend the network.

The main elements for maintaining a secure network and preventing network security attacks are security conscious personnel, security policies, management of vulnerabilities, and mitigation of threats. Conducting security education awareness results in an organization-wide security culture where individuals are cognizant of potential threats and understand the need for fast responsive action. Security policies provide the structure for permitted activity and security-focused procedures, and guiding personnel behavior via codes of ethics. Recommended security management procedures can be found in international standards and best practice guides provided by statutory agencies and network security organizations.

Performing risk analysis and the implementation and monitoring of countermeasures to address threats contributes significantly to the ongoing security of the network. Understanding the organization's vulnerabilities and the threats it faces provides the foundation for implementation of appropriate and cost-effective security measures. Organizations rely on computer networks for the majority of their day-to-day operations, and specific network security countermeasures provide protection for critical information assets. Numerous international risk management standards and guidelines are available to direct an organization's risk management process.

A solid approach to security incident handling provides the organization with a planned set of actions in response to intrusions. Guidelines for managing security incidents

recommend approved courses of action in dealing with attacks on critical assets. Prevention mechanisms complete the network security manager's toolkit in the quest to protect not only the organization's valuable information but also its own survivability.

References

1. Caralli, R.A., Stevens, J.F., Young, L.R., and Wilson, W.R., Introducing OCTAVE Allegro: Improving the information security assessment process, *Technical Report CMU/SEI-007-TR-012*, Carnegie Mellon University, Pittsburgh, PA, 2007.
2. CERT, Targeted cyber intrusion, mitigation strategies matrix, Computer Emergency Response Team and Defense Signals Directorate, Australian Government, 2009. http://www.cert.gov.au/www/cert/cert.nsf/Page/Alerts_and_Advisories, (accessed March 31, 2011.)
3. Defense Signals Directorate, *Australian Government Information Security Manual*, Australian Government, Department of Defense, Intelligence and Security, 2009. <http://www.dsd.gov.au/library/infosec/ism/index.html> (accessed March 31, 2011.)
4. IEEE Computer Society, *IEEE ISO/IEC Standard 16085-2006 Systems and Software Engineering—Life Cycle Processes—Risk Management*, ISO, Geneva, Switzerland and IEEE Standards Association, NJ, 2006.
5. ISACA, *The Risk IT Framework*, Information Systems Audit and Control Association, Rolling Meadows, IL, 2009.
6. ISO, *ISO 31000:2009 Risk Management Principles and Guidelines*, International Organization for Standardization, 2009. <http://www.iso.org>
7. ISO/IEC, *ISO/IEC 27000:2009 Information Security Management Systems*, International Organization for Standardization, 2009. <http://www.iso.org>, (accessed March 31, 2011.)
8. Scarfone, K., Grance, T., and Masone K., *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, NIST Special Publication 800-61, Gaithersburg, MD, 2008. <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>, (accessed March 31, 2011.)
9. Weaver, R., *Guide to Network Defense and Countermeasures*, Thomson Course Technology, Boston, MA, 2007.